



CVE-2019-14452

Published on: 07/30/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:58 PM UTC

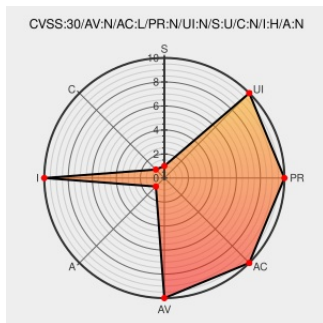
CVE-2019-14452

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Sigil before 0.9.16 is vulnerable to a directory traversal, allowing attackers to write arbitrary files via a `../` (dot dot slash) in a ZIP archive entry that is mishandled during extraction.

CVE-2019-14452 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
further harden against malicious epub and produce error message · Sigil-Ebook/Sigil@04e2f28 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/Sigil-Ebook/Sigil/commit/04e2f280cc4a0766bedcc7b9eb56449ceecc2ad4

Zip Slip in Sigil (CVE-2019-14452) – Mike Salvatore's Blog	salvatoresecurity.com text/html	 MISC salvatoresecurity.com/zip-slip-in-sigil-cve-2019-14452/
USN-4085-1: Sigil vulnerability Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4085-1
harden plugin unzipping to zip-slip attacks · Sigil-Ebook/Sigil@0979ba8 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/Sigil-Ebook/Sigil/commit/0979ba8d10c96ebca330715bfd4494ea0e019a8f
do not allow zip files to have upward relative path sections · Sigil-Ebook/Sigil@369eebe · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/Sigil-Ebook/Sigil/commit/369eebe936e4a8c83cc54662a3412ce8bef189e4
Zip Slip Vulnerability in FlightCrew · Issue #52 · Sigil-Ebook/flightcrew · GitHub	Third Party Advisory github.com text/html	 MISC github.com/Sigil-Ebook/flightcrew/issues/52#issuecomment-505997355
Release Sigil-0.9.16 · Sigil-Ebook/Sigil · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/Sigil-Ebook/Sigil/releases/tag/0.9.16
Zip Slip Vulnerability in FlightCrew · Issue #52 · Sigil-Ebook/flightcrew · GitHub	Third Party Advisory github.com text/html	 MISC github.com/Sigil-Ebook/flightcrew/issues/52#issuecomment-505967936
Comparing ea7f27d...5b867e5 · Sigil-Ebook/Sigil · GitHub	Third Party Advisory github.com text/html	 MISC github.com/Sigil-Ebook/Sigil/compare/ea7f27d...5b867e5

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Application	Flightcrew Project	Flightcrew	All	All	All	All

Application	Flightcrew Project	Flightcrew	All	All	All	All
Application	Sigil-ebook	Sigil	All	All	All	All
Application	Sigil-ebook	Sigil	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:19.04.*.*.*.*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:19.04.*.*.*.*.*.*:						
cpe:2.3:a:flightcrew_project:flightcrew:*.*.*.*.*:sigil:*.*:						
cpe:2.3:a:flightcrew_project:flightcrew:*.*.*.*.*:sigil:*.*:						
cpe:2.3:a:sigil-ebook:sigil:*.*.*.*.*.*.*:						
cpe:2.3:a:sigil-ebook:sigil:*.*.*.*.*.*.*:						

No vendor comments have been submitted for this CVE